What is claimed is:

1. A system for processing e-mail comprising:

a distributed network including a plurality of servers that receive e-mail messages for a plurality of different remotely located clients, each of the servers having a packet sniffer that extracts originating IP addresses associated with e-mail messages that are communicated to the clients over the network; and

a monitor that communicates with the packet sniffers and that monitors data regarding the originating IP addresses, determines whether traffic from an originating IP address has exceeded a threshold value, and generates a response for use in detecting spam e-mail messages if the threshold value has been exceeded.

2. The system of claim 1 wherein each of the servers further includes a blacklist containing IP addresses that have been determined to be generating spam e-mail messages; and

wherein each server checks the originating IP addresses of incoming connections to the addresses contained in the blacklist, and rejects any connection originating from an address on the blacklist.

3. The system of claim 1 wherein each of the servers further includes a message switch that determines whether e-mail messages are spam, and communicates e-mail messages to clients.

4. The system of claim 1 wherein the monitor resides on a server separate from the packet sniffers.

5. The system of claim 3 further comprising:

a spam database for storing rules for determining whether e-mail messages are spam;

wherein the message switch determines whether e-mail messages are spam based on the rules within the spam database.

6. The system of claim 5 wherein each rule in the database is assigned a score that is used to determine whether an e-mail message is spam.

7. The system of claim 6 wherein the response generated by the monitor comprises raising the score of a rule corresponding to the originating IP address.

8. The system of claim 1 wherein the response generated by the monitor comprises an alert that is communicated to a spam analyst.

9. The system of claim 2 wherein the response generated by the monitor comprises a command to add the originating IP address to the blacklist.

10. The system of claim 1 wherein the threshold value comprises a rate parameter.

11. The system of claim 1 wherein the threshold value comprises a maximum total connections parameter.

12. The system of claim 1 wherein the monitor determines whether an originating IP address has exceeded a threshold value by use of a token bucket algorithm including a rate parameter and a maximum connections allowed parameter.

13. A system for detecting spam e-mail messages in a distributed network including a plurality of servers that receive and process e-mail messages for a plurality of different remotely located clients, the system comprising:

a plurality of packet sniffers, each of which is located on a unique one of the plurality of servers and extracts originating IP addresses associated with e-mail messages that are communicated to clients by the server; and

a monitor that communicates with the packet sniffers and that monitors data regarding originating IP addresses, determines whether traffic from an originating IP address has exceeded a threshold value, and generates a response for use in detecting spam e-mail messages if the threshold value has been exceeded.

14. The system of claim 13 wherein the monitor resides on a server separate from the packet sniffers.

15. The system of claim 13 further comprising:

a blacklist stored on each of the servers, the blacklist including IP addresses that have been determined to be generating spam.

16. The system of claim 13 further comprising:

a spam database that stores rules for determining whether e-mail messages are spam; and

a message switch that determines whether e-mail messages are spam based on the rules within the spam database.

17. The system of claim 16 wherein each rule in the database is assigned a score that is used to determine whether an e-mail message is spam.

18. The system of claim 17 wherein the response generated by the monitor comprises raising the score of a rule corresponding to the originating IP address.

19. The system of claim 13 wherein the response generated by the monitor comprises an alert that is communicated to a spam analyst.

20. The system of claim 13 wherein the response generated by the monitor comprises a command to the system to block future e-mail messages from the originating IP address.

21. The system of claim 13 wherein the threshold value comprises a rate parameter.

22. The system of claim 13 wherein the threshold value comprises a maximum total connections parameter.

23. The system of claim 13 wherein the monitor determines whether traffic from an originating IP address has exceeded a threshold value by use of a token bucket algorithm including a rate parameter and a maximum connections allowed parameter.

24. A method for processing e-mail and detecting spam e-mail messages, comprising:

routing the e-mail messages through a distributed network including a plurality of servers that receive and process e-mail messages for a plurality of different remotely located clients;

communicating the processed messages to the plurality of remotely located clients by use of the plurality of servers;

extracting originating IP addresses associated with e-mail messages that are communicated to the plurality of remotely located clients;

monitoring data regarding originating IP addresses;

determining whether traffic from an originating IP address has exceeded a threshold value; and

generating a response for use in detecting spam e-mail messages if the threshold value has been exceeded.

25. The method of claim 24 further comprising:

storing data regarding the originating IP addresses in a database.

26. The method of claim 24 further comprising:

maintaining a list of acceptable IP addresses;

checking originating IP addresses against the list; and

determining whether traffic from an originating IP address has exceeded a threshold value only if the originating IP address is not in the list.

27. The method of claim 24 wherein the threshold value comprises a rate parameter.

28. The method of claim 24 wherein the threshold value comprises a maximum total connections parameter.

29. The method of claim 24 wherein determining whether traffic from an originating IP address has exceeded a threshold value is performed by use of a token bucket algorithm including a rate parameter and a maximum connections allowed parameter.

30. The method of claim 24 further comprising:

storing IP addresses that have been determined to be generating spam in a blacklist;

checking originating IP addresses of incoming connections to the servers against the IP addresses contained in the blacklist; and

rejecting any connection originating from an IP address in the blacklist.

31. The system of claim 30 wherein the response generated by the monitor comprises a command to add the originating IP address to the blacklist.

32. The method of claim 24 further comprising:

storing rules for determining whether e-mail messages are spam in a spam database; and

determining whether e-mail messages are spam based on the rules within the spam database.

33. The method of claim 32 wherein each rule in the database is assigned a score that is used to determine whether an e-mail message is spam.

34. The method of claim 33 wherein generating a response comprises raising the score of a rule corresponding to the originating IP address.

35. The method of claim 24 wherein generating a response comprises communicating an alert to a spam analyst.

36. The system of claim 24 wherein the response generated by the monitor comprises a command to the system to block future e-mail messages from the originating IP address.